Estructures Algebraiques: Tema 1

Dean

December 13, 2017

Contents

1 TODO Grup

2 TODO Interseccio, unio, producte i generacio

3 Elements d'un grup

3.1 Definicio Centre

Sigui G un grup, llavors el Centre G es $\mathcal{Z}(G) = \{a \in G \mid aba^{-1} = b \quad \forall b \in G\} = \{a \in G \mid ab = ba \quad \forall b \in G\}$.

3.2 Definicio Centralitzador

Sigui G un grup, i H un subgrup de G llavors el Centralitzador de H en G es $\mathcal{Z}_G(H) = \{a \in G \mid aba^{-1} = b \quad \forall b \in H\} = \{a \in G \mid ab = ba \quad \forall b \in H\}$.

3.3 Definicio Normalitzador

Sigui G un grup, i H un subgrup de G, llavors el normalitzador de H en G es $\mathrm{N_G(H)} = \{a \in G \mid aHa^{-1} = H\} = \{a \in G \mid aH = Ha\}$.

3.3.1 Observacio:

Normalitzador de H en G = G $\iff H \lhd G$

4 TODO Ordre d'un element, grup ciclic

5 TODO Morfismes de grups

6 Classes laterals

6.1 Definicio

Sigui G un grup i H in subgrup de G. $a, b \in G$.
Definim $a \sim b(esquerra) \iff a^{-1}b \in H$

6.2 Definicio de la classe d'equivalencia

$\bar{a} := \{\ b \in G \mid a \sim b\}$
$aH := \{\ ax \mid x \in H\}$
Observem que aH $=$ $\bar{a}$
A més H i aH tenen el mateix cardinal.

6.3 Definicio Classe Lateral:

Anomenem $G/H = \{aH|a \in G\}$ el conjunt de les classes laterals per l'esquerra (conjunt quocient).
Diem també que l'índex de H en G es $[G : H] = |G/H|$ $=$ nombre d' elements de G modul H

6.3.1 Observacio:

1. El nombre de classes laterals per l'esquerra es el mateix que el nombre de classes laterals per la dreta.

2. L'índex és multiplicatiu. K $\subset$ H $\subset$ G. Llavors [G:K] $=$ [G:H] * [H:K]

6.4 Teorema de Lagrange

Sigui G un grup i H un subgrup, G finit.
Aleshores $|G| = |G/H| * |H| \iff |G/H| = \frac{|G|}{|H|}$, i a més |H| divideix |G|.

6.4.1 TODO Demo

7 Subgrup normal, Grup quocient

7.1 Definicio: Subgrup Normal

Sigui G un grup, H un subgrup de G. H és subgrup normal de G si aH $=$ Ha $\forall$ a $\in$ G.

7.2 Lema

f: $G_1 \to G_2$ morfime de grups. Aleshores,

1. Si $H_1 \lhd G1 \implies f(H_1) \lhd f(G_1)$.

2. Si $H_2 \lhd G2 \implies f^{-1}(H_2) \lhd G_1$.

7.2.1 TODO Demo

7.3 Observacio

$H \subseteq K \subseteq G$, H,K subgrups de G. Aleshores.
Si $H \lhd G \implies H \lhd K$. El reciproc es fals.

7.4 Observacio

si $H \lhd G$, aleshores (aH)*(bH) = (ab)H

7.5 Definicio: Operacio interna

Sigui $H \lhd G$ i sigui G/H = {aH | a ∈ G} el conjunt de classes laterals per l'esquerra modul H. En G/H definim l'operacio interna:

$$\begin{aligned} G/H \times G/H &\to G/H \\ aH \times bH &\mapsto (ab)H \end{aligned}$$

7.6 Corol.lari

G/H es un grup i s'anomena el grup quocient de G per H.

7.7 Exercici: La aplicacio quocient es un morfisme

8 Primer teorema d'isomorfisme

8.1 TODO Teorema:

Sigui $f : G_1 \to G_2$ morfisme de grups, Sigui $H \lhd G_1$, i sigui l'aplicació

$$\begin{aligned} \tilde{f} : G_1/H &\to G_2 \\ aH &\mapsto \tilde{f}(aH) := f(a) \end{aligned}$$

9 El grup multiplicatiu d'un cos finit

9.1 Definicio

Sigui $\mathbb{K}$ un cos. El grup multiplicatiu de $\mathbb{K}$ és

$$\mathbb{K}^* = \mathbb{K} \setminus \{0\} = \{x \in \mathbb{K} \mid x \neq 0\}$$

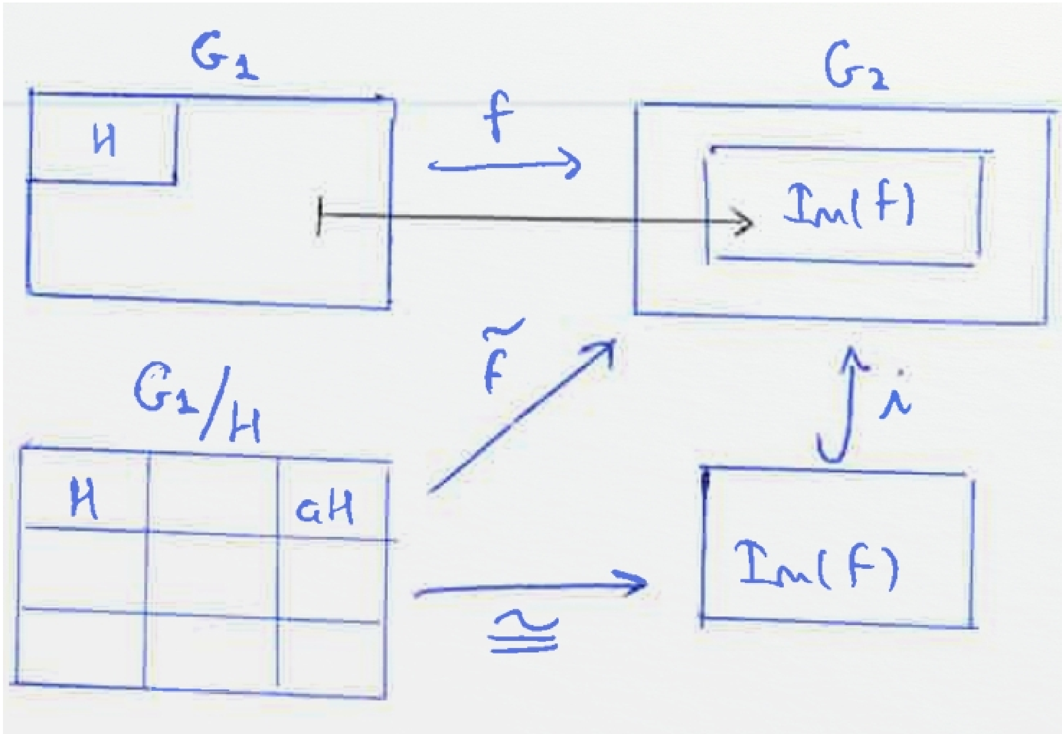

Figure 1: Primer teorema d'isomorfisme

9.2 Teorema

Sigui $\mathbb{K}$ un cos. Sigui G un subgrup finit de $\mathbb{K}^*$. Aleshores G és cíclic

9.2.1 TODO demo

10 Grup simples

10.1 Definicio

Sigui G un grup no trivial. Direm que G es simple si els unics subgrups normals de G son $\{1\}$ i G.

10.2 Proposicio

Sigui G un grup no trivial. Son equivalents

1. G es simple i abelia
2. $|\mathrm{G}| = \mathrm{p}$, on p es primer
3. $G \cong \mathbb{Z}/p\mathbb{Z}$

10.2.1 TODO Demo

10.3 Teorema de Feit-Thompson

Sigui G grup simple, Suposem |G| es senar. Aleshores G es ciclic i $G \cong \mathbb{Z}/p\mathbb{Z}$.

10.4 Teorema

Sigui n $\geq$ 5, Aleshores $\mathcal{A}_n$ es simple

10.4.1 TODO Demo

10.5 Proposicio

Sigui G un grup, $H \lhd G$. Aleshores,
G/H es grup simple $\iff$ H es un element maximal en el conjunt {K | $K \lhd G$, $K \neq G$}

10.5.1 TODO Demo

11 Grup resolubles

11.1 Definicio torre normal

Una torre normal de G es $G = G_0 \rhd G_1 \rhd G_2 \rhd \ldots \rhd G_n = \{1\}$ on G es un grup i $G_i \lhd G_{i+1}$.
Anomenem n la *longitud de la torre*
G_{i-1}/G_i s'anomenen els *quocients de la torre*

A mes definim:

- **Torre normal abeliana**: Torre normal amb quocients abelians.
- **Torre normal simple/serie de composicio**: Torre normal amb quocients abelians

11.2 Definicio Grup Resoluble

Direm que G es resoluble si te una torre normal abeliana.

11.3 Teorema: Segon Teorema d'isomorfisme

Sigui G grup i H,K dos subgrups de G. Suposem $H \lhd G$. Aleshores:

1. $H \cap K \lhd K$
2. $H \cdot K$ es subgrup de G
3. $H \lhd H \cdot K$
4. A mes a mes, ${}^{K}/_{H \cap K} \cong {}^{H \cdot K}/_{H}$

11.3.1 TODO Demo

11.4 Teorema: Jordan-Holder

Sigui G un grup i $\left\{ \begin{array}{l} G = G_0 \rhd G_1 \rhd G_2 \rhd \ldots \rhd G_n = \{1\} \\ G = H_0 \rhd H_1 \rhd H_2 \rhd \ldots \rhd H_m = \{1\} \end{array} \right\}$ Dues series de composicio de G

Aleshores n = m, i $\exists \sigma \in \mathcal{S}_n$ tal que ${}^{H_i}/_{H_{i+1}} \cong {}^{G_{\sigma(i)}}/_{G_{\sigma(i)+1}}$.

11.4.1 TODO Demo

11.5 Proposicio

Sigui G un grup, H un subgrup de G. Aleshores

1. Si G es resoluble $\implies$ H es resoluble
2. Si $H \lhd G$ i G es resoluble $\implies$ ${}^{G}/_{H}$ es resoluble
3. Si $H \lhd G$ i H i ${}^{G}/_{H}$ son resolubles $\implies$ G es resoluble

12 Accio d'un grup en un conjunt

12.1 Definicio: Accio d'un grup en un conjunt

Sigui G un grup. SIgui X un conjunt. Una accio de G en X es una aplicacio

$$\begin{aligned} \varphi : G \times X &\to X \\ (a, x) &\mapsto \varphi(a, x) = ax \end{aligned}$$

tal que:

1. $a \cdot (b \cdot x) = (a \cdot b) \cdot x \quad \forall a, b \in G, \forall x \in X$
2. $1 \cdot x = x \quad \forall x \in X$

12.2 Observacio

Hi ha una bijeccio entre
$\{\varphi : G \times X \to X \mid \varphi$ accio de G en X$\} \leftrightarrow \{\phi : G \to Perm(X) \mid \phi$ morfisme de grups$\}$

12.3 Definicio: Orbita d'un element

L'orbita de $x \in X$ es el subconjunt $G \cdot x = \{ax \mid a \in G\} \subseteq X$

12.4 Definicio: L'estabilitzador/grup d'isotropia d'x $\in$ X

Gx $:= \{a \in G \mid ax = x\} \subseteq G$, es un subgrup de G.

12.5 Lema:

Si x,y estan en la mateixa orbita, els seus estabilitzadors son conjugats.
Concretament, si y = ax $\implies$ $G_y = aG_xa^{-1}$

12.5.1 TODO DEMO

12.6 Proposicio

L'aplicacio

$$G \cdot x \to {}^{G}/_{G_x}$$
$$ax \mapsto a \cdot G_x$$

esta ben definida i es bijectiva. En particular,

1. $|G \cdot x| = |{}^{G}/_{G_x}| = [G : G_x]$
2. Si G es finit, $|G \cdot x| \big| |G|$
3. Si X es finit, $|X| = \sum_{i=1}^{n} |G \cdot x_i| = \sum_{i=1}^{n} [G : G_{x_i}]$

12.6.1 TODO DEMO

12.7 Definicio: punt fix

$x \in X$ es un punt fix per l'accio si ax = x $\forall a \in G$. En particular
$G \cdot x = \{ax \mid a \in G\} = \{x\}$, $G_x = \{a \in G \mid ax = x\} = G$

12.8 Definicio: Accio Transitiva

$G \times X \to X$ es accio transitiva si $\forall$ x,y $\in$ X, $\exists$ a $\in$ G tal que y = ax.
En aquest cas. G $\cdot$ y = X $\forall$ y $\in$ X.

12.9 Definicio: Accio Fidel

$G \times X \to X$ es accio fidel si $\forall$ a $\neq$ b, a,b $\in$ G. Aleshores $\mathrm{m_a} \neq \mathrm{m_b}$, on

$$m_a : X \to X$$
$$x \mapsto ax$$

$\mathrm{m_a} \in$ Perm(x)

12.9.1 Observacio:

Si be $G \times X \to X \cong m : G \to Perm(x)$ es morfisme de grups, si imposem que es fidel, el morfisme es injectiu. A mes si X es finit l'accio es isomorf a un subgrup del grup simetric.

12.10 Accio per translacio en X, quan X = G

Sigui G un grup, definim

$$G \times G \to G$$
$$a \quad x \mapsto a \cdot x = ax$$

I es efectivament una accio.

12.11 Teorema de Cayley

Sigui G un grup finit, n = |G|. Aleshores G es isomorf a un subgrup del grup simetric $\mathcal{S}_n$

12.11.1 TODO Demo

12.12 Definicio: Accio per conjugacio de G en X = G

$$\begin{aligned} G \times G &\to G \\ a \quad x &\mapsto a \cdot x = axa^{-1} \end{aligned}$$

12.12.1 Centre

$x \in G$ es punt fix $\iff a \cdot x = x \quad \forall a \in G \iff axa^{-1} = x \forall a \in G \iff ax = xa \quad \forall a \in G \iff x \in \mathcal{Z}(G) = \{x \in G \mid ax = xa \quad \forall a \in G\} =$ centre de G. El centre de G es subgrup.

12.12.2 Centralitzador

L'estabilitzador de y ∈ G es $G_y = \{a \in G \mid a \cdot y = y\} = \{a \in G \mid aya^{-1} = y\} = \{a \in G \mid ay = ya\} = \mathcal{Z}_G(y)$, centralitzador de G. El centralitzador tambe es un subgrup de G.

12.13 Definicio: Accio per translacio en les classes laterals

Sigui G grup, H subgrup de G i X = $G/H = \{aH \mid a \in G\}$

$$\begin{aligned} G \times G/H &\to G/H \\ a \quad bH &\mapsto abH \end{aligned}$$

- Es una accio transitiva.
- si $aH \in X = G/H$: L'estabilitzador de aH es $G_{aH} = \{b \in G \mid b(aH) = aH\} = aHa^{-1}$

12.14 Definicio: Accio per conjugacio en els subgrups

Sigui G grup i $X = \{H \mid$ H subgrup de G$\}$.

$$\begin{aligned} G \times \{\text{sg. de G}\} &\to \{\text{sg. de G}\}, \text{ conjugat de H} \\ a \qquad H &\mapsto aHa^{-1} \end{aligned}$$

Si H es subgrup de G, l'orbita d'H es:
$G \cdot H = \{a \cdot H \mid a \in G\} = \{aHa^{-1} \mid a \in G\}$: els conjugats de H

H es punt fix per l'accio si $a \cdot H = H \iff aHa^{-1} = H \quad \forall a \in G \iff$ H es subgrup normal de G

L'estabilitzador de H es: $G_H = \{a \in G \mid a \cdot H = H\} = \{a \in G \mid aHa^{-1} = H\} = N_G(H)$: Normalitzador de H en G

Sabem que $|G \cdot H| = [G : G_H]$. Per tant.
$H \lhd G \iff$ H es punt fix per l'accio $\iff$ L'orbita de H te un sol punt $\iff |G \cdot H| = 1 \iff [G : G_H] = 1 \iff G_H = G \iff N_G(H) = G$

12.15 Teorema de Cauchy

Sigui G un grup finit, |G| = n. Sigui p primer tal que p|n.
ALeshores, ∃ x ∈ G tal que ord(x) = p

12.15.1 TODO Demo

13 Subgrups de Sylow

13.1 Definicio: p-grups: Subgrups de Sylow

Sigui G un grup i p un nombre primer. Aleshores, G es un p-grup $\iff$ $|G| = p^r$ per a algun r ≥ 0.

13.2 Teorema:

Sigui G un p-grup. Aleshores, |G| = p^{r}, r ≥ 0, i:

1. G no trivial $\iff$ $\mathcal{Z}(G)$ no trivial.
2. G es resoluble
3. si G es simple, aleshores G ≅ $\mathbb{Z}/p\mathbb{Z}$

13.2.1 TODO demo

14 Teoremas de Sylow

14.1 Teorema: Primer Teorema de Sylow

Sigui G un grup finit i considerem p primer, r ≥ 0.
Aleshores, si $p^r \big| |G| \implies G$ conte un subgrup d'ordre p^r

14.2 Definicio

Sigui G grup finit, $|G| = p^r \cdot m$, p primer, r ≥ 0, p ∤ m.
Denotem $\mathrm{S_yl_p}$(G) = $\{H$ | H subgrup de G, $|H| = p^r\}$.
Els anomenem els p-subgrups de Sylow de G (p-Sylow de G) i denotem $\mathrm{n_p}$(G) = cardinal de $\mathrm{S_yl_p}$(G).

14.2.1 Observacio:

1. El conjugat d'un p-Sylow es un p-Sylow ja que $|H| = |aHa^{-1}|$.
2. Els P-subgrups son $\{H$ | H subgrup de G, $|H| = p^s, s \leq r\}$.

14.3 Teorema: Segon Teorema de Sylow

Sigui G grup finit, $|G| = p^r \cdot m$, p primer, r $\geq$ 0, p $\nmid$ m.

1. Si L es un p-subgrup de G ($|L| = p^s, s \leq r$). Aleshores $\exists H \in S_y l_p(G)$ tal que $L \subseteq H$
2. Si H i P son dos p-Sylow de G. Aleshores $\exists a \in G$ tal que $aHa^{-1} = P$., Es a dir, tots els p-Sylow son conjugats.
3. $\mathrm{n_p(G)} \equiv 1 \pmod{\mathrm{p}}$ i $\mathrm{n_p(G)|m}$.

14.3.1 TODO Demo